FORM-PTO-1390 (Rev. 9-2001) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE **TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371**		ATTORNEY'S DOCKET NUMBER 032326-192 U.S APPLICATION NO. (If known, see 37 C F.R. 1.5) Unassigned 10/048216
INTERNATIONAL APPLICATION NO. PCT/FR00/02024	INTERNATIONAL FILING DATE 12/07/2000	PRIORITY DATE CLAIMED 30/07/1999

TITLE OF INVENTION
SIGNATURE SCHEMES BASED ON DISCRETE LOGARITHM WITH PARTIAL OR TOTAL MESSAGE RECOVERY

APPLICANT(S) FOR DO/EO/US
Jean-Sébastien CORON, David NACCACHE and Jacques STERN

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below.
4. ☐ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is attached hereto (required only if not communicated by the International Bureau).
   b. ☒ has been communicated by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☒ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are attached hereto (required only if not communicated by the International Bureau).
   b. ☐ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ An English language translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 20 below concern document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A FIRST preliminary amendment.
14. ☐ A SECOND or SUBSEQUENT preliminary amendment.
15. ☐ A substitute specification.
16. ☐ A change of power of attorney and/or address letter.
17. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
18. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
19. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. ☐ Other items or information:

21839

U.S. APPLICATION NO. (If known, see 37 C.F.R. 1.5) Unassigned	10/048216	INTERNATIONAL APPLICATION NO. PCT/FR00/02024	ATTORNEY'S DOCKET NUMBER 032326-192

21. ☒ The following fees are submitted:				CALCULATIONS	PTO USE ONLY
Basic National Fee (37 CFR 1.492(a)(1)-(5)): Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO .... $1,040.00 (960) International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO .... $890.00 (970) International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO .... $740.00 (958) International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) .... $710.00 (956) International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) $100.00 (962)					
ENTER APPROPRIATE BASIC FEE AMOUNT =				$ 890.00	
Surcharge of **$130.00 (154)** for furnishing the oath or declaration later than 20 □ 30 □ months from the earliest claimed priority date (37 CFR 1.492(e)).				$ -0-	
Claims	Number Filed	Number Extra	Rate		
Total Claims	30 -20 =	10	X$18.00 (966)	$ 180.00	
Independent Claims	8 -3 =	5	X$84.00 (964)	$ 420.00	
Multiple dependent claim(s) (if applicable)			+$280.00 (968)	$ -0-	
TOTAL OF ABOVE CALCULATIONS =				$ 1,490.00	
Reduction for 1/2 for filing by small entity, if applicable (see below). +				$ -0-	-
SUBTOTAL =				$ 1,490.00	
Processing fee of **$130.00 (156)** for furnishing the English translation later than 20 □ 30 □ months from the earliest claimed priority date (37 CFR 1.492(f)). +				$ -0-	
TOTAL NATIONAL FEE =				$ 1,490.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00 (581)** per property +				$ -0-	
TOTAL FEES ENCLOSED =				$ 1,490.00	
				Amount to be refunded:	$
				charged:	$

a. □ Small entity status is hereby claimed.

b. ☒ A check in the amount of $ 1,490.00 to cover the above fees is enclosed.

c. □ Please charge my Deposit Account No. 02-4800 in the amount of $______ to cover the above fees. A duplicate copy of this sheet is enclosed.

d. □ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 02-4800. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

James A. LaBarre
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

SIGNATURE

James A. LaBarre
NAME

28,632
REGISTRATION NUMBER

January 30, 2002
DATE

Patent
Attorney's Docket No. 032326-192

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of)
)
Jean-Sébastien CORON et al) Group Art Unit: Unassigned
)
Application No.: Unassigned) Examiner: Unassigned
)
Filed: January 30, 2002)
)
For: A SMART CARD ARCHITECTURE)
INTEGRATING PERIPHERALS)

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Prior to examination and the calculation of filing fees, kindly amend the above-identified application as follows:

IN THE SPECIFICATION:

Page 1, immediately following the title appearing on line 1 and 2, insert the following:

--This disclosure is based upon French Application No. 99/10106, filed on July 30, 1999 and International Application No. PCT/FR00/02024, filed July 12, 2000, which was published on February 8, 2001 in a language other than English, the contents of which are incorporated herein by reference.

Background of the Invention--

Page 4, before line 6, insert the following heading:

--**Description of the Invention**--

Add the following Abstract:

--Signature scheme methods, in which security is based on the discrete logarithm problem, include a first scheme for total recovery of the message, and a second scheme for partial recovery of the message. Two techniques reduce to a minimum the total size of the message to be transmitted and the signature. In the first technique, part of the message is included inside the signature by appropriately selecting the random data used when the signature is generated. In the second technique, part of the octets representing the signature are eliminated and the total recovery of the signature is obtained during the second verification phase. These schemes and techniques reduce the overall size of the signature and the message to be transmitted. They are therefore particularly suitable for use on portable media such as smart cards.--

IN THE CLAIMS:

Kindly replace claims 1-25, as follows.

1. (Amended) An electronic signature method comprising a generation method and a verification method allowing total reconstitution of a message, said method utilising a redundancy function R, a set having a group structure of order r, where r is a prime number, with a zero element denoted O and generating the point G, and employing a private key that is a positive integer less than r, and a public key being the point W=s.G,

said method using a non-zero integer constant k, wherein the signature generation method includes the following four steps:

1) Generating a random number u between 1 and r-1 and calculating V=u.G;

2) Associating an integer i with the point V and calculating c=i+f modulo r; if c=0, returning to step 1;

3) Calculating the integer $d=u^{-1}*(k+s*c)$ modulo r; if d=0, returning to step 1; and

4) Utilizing the pair of integers (c,d) as the signature;

and wherein the signature verification method includes the following six steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [1,r-1], the signature is not valid;

2) Calculating the integers $h = d^{-1}$ modulo r, $h_1=k*h$ modulo r and $h_2=c*h$ modulo r;

3) Calculating the point $P = h_1G + h_2W$; if P=0, the signature is not valid;

4) Associating an integer i with the point P;

5) Calculating the integer f=c-i modulo r; and

6) Finding the message m from f and verifying that f=R(m); if yes, the signature of the message m is valid; otherwise the signature is not valid.

2. (Amended) An electronic signature method comprising a generation method and a signature verification method allowing partial reconstruction of a message, the message m to be signed being divided into two parts, the first part m_1 of constant size being

reconstituted from the signature, the second part m_2 being transmitted with the signature of the method, said method utilising a redundancy function R, a set having a group structure of order r, where r is a prime number, with a zero element denoted O and generating the point G, and employing a private key that is a positive integer less than r and a public key being the point W=s.G, wherein the method of generating the signature of a message m consisting of the messages m_1 and m_2 includes the following six steps:

1) Generating a random integer u between 1 and r-1 and calculating V=u.G;

2) Calculating $f_1=R(m_1)$;

3) Associating an integer i with the point V and calculating $c=i+f_1$ modulo r; if c=0, returning to step 1;

4) Calculating $f_2=H(m_2)$, where H is a hash function;

5) Calculating the integer $d=u^{-1}*(f_2+s*c)$ modulo r; if d=0, returning to step 1; and

6) Utilizing the pair of integers (c,d) as the signature;

and wherein the signature verification method takes as an input a pair of integers (c,d) and the partial message m_2 and comprises the following seven steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [1,r-1], the signature is not valid;

2) Calculating $f_2=H(m_2)$, where H is a hash function;

3) Calculating the integers $h=d^{-1}$ modulo r, $h_1=f_2*h$ modulo r and $h_2=c*h$ modulo r;

4) Calculating the point $P=h_1G+h_2W$; if P=0, the signature is not valid;

5) Associating the integer i with the point P;

6) Calculating the integer $f_1=c-i$ modulo r; and

7) Obtaining the message m_1 from f_1 and verifying that $f_1=R(m_1)$; if yes, the signature of the message m is valid; otherwise the signature is not valid.

3. (Amended) An electronic signature method comprising a generation method and a signature verification method that comprises including part of the message inside the signature by suitably choosing the random data used during the generation of the signature.

4. (Amended) An electronic signature method comprising a generation method and a signature verification method that comprises the steps of eliminating some of the bytes representing the signature, and reconstituting the signature during the verification phase.

5. (Amended) A method according to claim 3 for improving the Nyberg-Rueppel signature scheme, comprising a generation method and a verification method in which part of the message of size t bytes is included in the integer d, t being a small integer, the signature being a pair of integers (c,d), the t least significant bytes of an integer g containing t bytes of the message, the said method using a redundancy function R, a set having a group structure of order r, where r is a prime number, with a zero element denoted O and generating the point G, and employing a private key that is a positive integer

s less than r and a public key being the point $W=s.G$, wherein the method of generating the signature of a message m includes the following five steps:

1) Removing the t least significant bytes of the message m and storing the result in m'; calculating $f=R(m')$;

2) Generating a random number u between 1 and r-1 and calculating $V=u.G$;

3) Associating an integer i with the point V and calculating $c=i+f$ modulo r; returning to step 1 if $c=0$.

4) Calculating the integer $d=u-s*c$ modulo r; if d is not equal to m modulo 2^{8t}, returning to step 2; and

5) Utilizing the pair of integers (c,d) as the signature;

and wherein the signature verification method includes the following five steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [0,r-1], the signature is not valid;

2) Calculating the point $P=d.G+c.W$; if $P=0$, the signature is not valid;

3) Associating the integer i with the point P;

4) Calculating the integer $f=c-i$ modulo r;

5) Obtaining the message m' from f and verifying that $f=R(m')$; if such is not the case, the signature is not valid; if such is the case, the signature is valid and the message m is the concatenation with the message m' of the t least significant bytes of the integer d.

6. (Amended) A method according to claim 5 for the preprocessing of the signature generation to accelerate the generation of the signatures, said method comprising a pretreatment phase and a signature generation phase, said pretreatment phase taking as an input a secret key s and putting in memory in a table a large number of values (i, x_u) with x_u=u-s*i modulo r and i being the integer associated with the point V=u.G, so that these values can be accessed by the remainder of x_u modulo 2^{8t}, said signature generation phase utilising a redundancy function R, a set having a group structure of order r, where r is a prime number, with a zero element denoted O and generating the point G, and employing a private key that is a positive integer s less than r and a public key being the point W=s.G, said signature generation phase comprising the following eight steps:

1) Removing the t least significant bytes in the message m and storing the result in the message m'; calculating f=R(m'). The t least significant bytes of the message m are stored in the integer d;

2) Calculating the integer y=s*f modulo r and the integer 1=y modulo 2^{8t};

3) If y<r/2, first of all executing step 4 and next step 5; otherwise executing first of all step 5 and next step 4;

4) Accessing the elements of the table where the remainder modulo 2^{8t} is 1+d modulo 2^{8t} and selecting an element such that x_u is greater than or equal to y; if such an element exists, it is eliminated from the table and the method passes to step 6;

5) Accessing the elements of the table where the remainder modulo 2^{8t} is 1+d+r modulo 2^{8t} and selecting an element such that x_u is less than y; if such an element exists, it is eliminated from the table and the method passes to step 6;

6) Calculating the integer $d=x_u-y$ modulo r;

7) Obtaining the integer i associated with x_u and calculating $c=i+f$ modulo r;

and

8) Utilizing the pair of integers (c,d) as the signature.

7. (Amended) A method according to claim 2 for improving the signature scheme with partial reconstitution of the message, said method comprising a signature generation method and a signature verification method, said method including part of the message of size t bytes in the integer d, t being a small integer, the t least significant bytes of the integer d containing t bytes of the message, said method utilising a redundancy function R, a set having a group structure of order r, where r is a prime number, with a zero element denoted O and generating a point G, and employing a private key that is a positive integer less than r and a public key being the point W=s.G, wherein the method of generating the signature of a message m consisting of the messages m_1 and m_2 includes the following six steps:

1) Generating a random integer u between 1 and r-1 and calculating V=u.G;

2) Calculating $f_1=R(m_1)$;

3) Associating an integer i with the point V and calculating $c=i+f_1$ modulo r; if c=0, returning to step 1;

4) Calculating $f_2=H(m_2)$, where H is a hash function;

5) Calculating the integer $d=u^{-1}*(f_2+s*c)$ modulo r; if d=0 or if d is not equal to m_2 modulo 2^{8t}, returning to step 1; and

6) Utilizing the pair of integers (c,d) as the signature, and the message to be transmitted is m'_2 consisting of m_2 deprived of its t least significant bytes;

and wherein the signature verification method takes as an input a pair of integers (c,d) and the partial message m'_2 and comprises the following eight steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [1,r-1], the signature is not valid;

2) Making up m'_2 as m_2 by adding to it the t least significant bytes of d;

3) Calculating $f_2=H(m_2)$, where H is a hash function;

4) Calculating the integers $h=d^{-1}$ modulo r, $h_1=f_2*h$ modulo r and $h_2=c*h$ modulo r;

5) Calculating the point $P=h_1G+h_2W$; if $P=0$ the signature is not valid;

6) Associating the integer i with the point P;

7) Calculating the integer $f_1=c-i$ modulo r; and

8) Obtaining the message m_1 from $f_1$and verifying that $f_1=R(m_1)$; if yes, the signature of the message m is valid; otherwise the signature is not valid.

8. (Amended) A method that includes removing t bytes from a chain of bytes representing an integer d from a signature that is the pair of integers (c,d), said method comprising a signature generation method and a signature verification method, said method being applied to the Nyberg and Rueppel signature scheme, wherein the signature generation method includes the following two steps:

1) Generating the signature of the message m using the Nyberg and Rueppel signature scheme, to obtain the pair of integers (c,d); and

2) Calculating d', the integer quotient of the division of the integer d by 2^{8t}; and utilizing the pair of integers (c,d') as the signature;

and wherein the signature verification method takes as an input a pair (c,d') and includes the following five steps:

1) If c does not belong to the interval [1,r-1], the signature is not valid;

2) Calculating the point $P=d'*2^{8t}.G+c.W$;

3) For j ranging from 0 to $2^{8t}-1$, executing the following steps:

3a) If P=O, executing step 3d);

3b) Associating the integer i with the point P and calculating the integer f=c-i modulo r;

3c) Finding the message m from f and verifying that f=R(m); if yes, executing step 5;

3d) Replacing P with P+G;

4) The signature is not valid and the method is terminated;

5) If the integer $d=d'*2^{8t}+j$ does not belong to the interval [0,r-1], the signature is not valid; otherwise the signature is valid and the method is terminated.

9. (Amended) A method that includes removing t bytes from a chain of bytes representing an integer d from a signature that is the pair of integers (c,d), said method comprising a signature generation method and a signature verification method, with partial

reconstitution of a message according to Claim 2, wherein the signature generation method includes the following two steps:

1) Generating the signature of a message m using the signature scheme with partial reconstruction of the message according to claim 2, in order to obtain the pair of integers (c,d); and

2) Calculating d', the integer quotient of the division of the integer d by 2^{8t};

wherein the signature is the pair of integers (c,d');

and wherein the modified signature verification method takes as an input a pair (c,d') and a message m_2 and includes the following two steps:

1) For i ranging from 0 to 2^{8t}-1, calculating the integer $d=d'*2^{8t}+i$ and executing the signature verification method with partial reconstitution of the message according to claim 2, the signature to be verified being (c,d); if the signature verification method recognises the signature (c,d) as valid, the signature is valid, and the method is terminated;

2) Otherwise the signature is not valid.

10. (Amended) A method for improving the Nyberg and Rueppel scheme making it possible to increase the size of the messages to be signed by t bytes, t being an integer variable, said method comprising a signature generation method and a signature verification method, said method utilising a redundancy function R, a set having a group structure of order r, where r is a prime number, with a zero element denoted O and generating the point G, and employing a private key that is a positive integer s less than r

and a public key being the point W=s.G, wherein the method of generating the signature of a message m includes the following five steps:

1) Generating a random number u and calculating V=u.G;

2) Obtaining the message m' by removing from the message m the t least significant bytes and calculating f=R(m');

3) Associating an integer i with the point V and calculating c=i+f modulo r; returning to step 1 if c=0 and if i is not equal to m modulo 2^{8t};

4) Calculating d=u-s*c modulo r; and

5) Utilizing the pair of integers (c,d) as the signature;

and wherein the signature verification method includes the following four steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [0,r-1], the signature is not valid;

2) Calculating the point P=d.G+c.W; if P=O, the signature is not valid;

3) Associating the integer i with the point P and calculating the integer f=c-i modulo r; and

4) Finding the message m' from f and verifying that f=R(m'); if yes, finding the message m by concatenating the t least significant bytes of i with the message m'. The signature of the message m is then valid; otherwise the signature is not valid.

11. (Amended) A method for improving a signature scheme with partial reconstitution of the message according to Claim 2, said method comprising a signature generation method and a signature verification method, and making it possible to increase

by t bytes the size of the message m_1 reconstituted from the signature, t being an integer variable, said method utilising a redundancy function R, a set having a group structure of order r, where r is a prime number, with a zero element denoted O and generating the point G, and employing a private key that is a positive integer less than r and a public key being the point W=s.G, wherein the method of generating the signature of a message m includes the following six steps:

1) Generating a random integer u between 1 and r-1 and calculating V=u.G;

2) Obtaining m'_1 by removing the t least significant bytes from the message m_1. Calculating $f_1=R(m'_1)$;

3) Associating an integer i with the point V and calculating $c=i+f_1$ modulo r; if c=0 or if i is not equal to m_1 modulo 2^{8t}, returning to step 1;

4) Calculating $f_2=H(m_2)$, where H is a hash function;

5) Calculating the integer $d=u^{-1}*(f_2+s*c)$ modulo r; if d=0, returning to step 1; and

6) Utilizing the pair of integers (c,d) as the signature;

and wherein the signature verification method takes as an input a pair of integers (c,d) and the partial message m_2 and comprises the following seven steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [1,r-1], the signature is not valid;

2) Calculating $f_2=H(m_2)$, where H is a hash function;

3) Calculating the integers $h=d^{-1}$ modulo r, $h_1=f_2*h$ modulo r and $h_2=c*h$ modulo r;

4) Calculating the point $P=h_1G+h_2W$; if $P=O$, this signature is not valid.

5) Associating the integer i with the point P;

6) Calculating the integer f_1=c-i modulo r; and

7) Obtaining the message m'_1 from f_1 and verifying that $f_1=R(m'_1)$; if yes, obtaining m_1 by concatenating the t least significant bytes of the integer i with the message m'_1. The signature of the message m is then valid; otherwise the signature is not valid.

12. (Amended) A method according to claim 11 for preprocessing the calculations making it possible to increase performance, comprising the further step of putting in memory in a table the pairs of integers (u,i) so that these integers are accessible to the value of i modulo 2^{8t}, t being an integer parameter.

13. (Amended) A method for improving the Nyberg and Rueppel signature scheme consisting in removing t bytes from an integer c, t being an integer variable, said method comprising a signature generation method and a signature verification method, the signature consisting of the pair of integers (c,d), wherein the signature generation method includes the following two steps:

1) Generating the signature of a message m using the Nyberg-Rueppel signature scheme in order to obtain the pair of integers (c,d); and

2) Calculating c', the integer quotient of the division of the integer c by 2^{8t}, and employing the pair of integers (c',d) as the signature;

and wherein the signature verification method takes as an input the pair of integers (c',d) and includes the following five steps:

1) If d does not belong to the interval [0,r-1], the signature is not valid;

2) Calculating the point $P=d.G+c'*2^{8t}.W$;

3) For j ranging from 0 to $2^{8t}-1$, executing the following steps:

3a) If P=O, executing step 3d);

3b) Associating the integer i with the point P and calculating the integer f=c-i modulo r;

3c) Finding the message m from f and verifying that f=R(m); if yes, executing step 5;

3d) Replacing P by P+W;

4) The signature is not valid and the method is terminated;

5) If the integer $c=c'*2^{8t}+j$ does not belong to the interval [1,r-1], the signature is not valid; otherwise the signature is valid and the method is terminated.

14. (Amended) A method according to claim 2 for improving the signature scheme with partial reconstitution of the message that includes the further step of removing t bytes from the integer c, t being an integer variable, said method comprising a signature generation method and a signature verification method, wherein the signature generation method comprises the following two steps:

1) Generating the signature of the message m, using the signature scheme with partial reconstitution of the message in order to obtain the pair of integers (c,d); and

2) Calculating c', the integer quotient of the division of the integer c by 2^{8t}; and utilizing the pair of integers (c',d) as the signature;

and wherein the signature verification method takes as an input a pair of integers (c',d) and a message m_2 and comprises the following eight steps:

1) If d does not belong to the interval [1,r-1], the signature is not valid;

2) Calculating $f_2=H(m_2)$, where H is a hash function;

3) Calculating the integers $h=d^{-1}$ modulo r, $h_1=f_2*h$ modulo r and $h_2=c'*2^{8t}*h$ modulo r;

4) Calculating the point $P=h_1.G+h_2.W$;

5) Calculating the point $Z=h.W$;

6) For j ranging from 0 to $2^{8t}-1$, executing the following steps:

6a) If P=O, executing step 6d);

6b) Associating the integer i with the point P and calculating the integer $f_1=c-i$ modulo r;

6c) Finding the message m_1 from f_1 and verifying that $f_1=R(m_1)$; if yes, executing step 8;

6d) Replacing P with P+Z;

7) The signature is not valid and the method is terminated;

8) If the integer $c=c'*2^{8t}+j$ does not belong to the interval [1,r-1], the signature is not valid; otherwise the signature is valid and the method is terminated.

15. (Amended) A method according to claim 1 for modifying the signature scheme with partial reconstruction of the message comprising the further step of replacing the signature (c,d) with the signature (h_2,d) with $h_2=c*d^{-1}$ modulo r.

16. (Amended) A method for improving the Nyberg-Rueppel signature scheme, said method comprising a signature generation method and a signature verification method, the said method having the step of including part of a message of size t bytes in an integer d, the signature being the pair of integers (c,d), t being a small integer, the t least significant bytes of the integer d containing t bytes of the message, the said method utilising a set having a group structure of order r, where r is a prime number, with a zero element denoted O and generating the point G, and employing a private key that is a positive integer s less than r and a public key being the point W=s.G, wherein the method of generating the signature of a message m using the integer parameters t, a and k includes the following seven steps:

1) Calculating h=H(m), H being a hash function;

2) Removing the t least significant bytes and the k most significant bytes of the message m and storing the result in m';

3) Storing as f the result of the concatenation with m' of the a most significant bytes of h;

4) Generating a random number u between 1 and r-1 and calculating V=u.G;

5) Associating an integer i with the point V and calculating c=i+f modulo r; returning to step 4 if c=0;

6) Calculating the integer d=u-s*c modulo r; if d is not equal to m modulo 2^{8t} returning to step 4; and

7) Utilizing the pair of integers (c,d) as the signature;

and wherein the signature verification method includes the following seven steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [0,r-1], the signature is not valid;

2) Calculating the point P=d.G+c.W; if P=O, the signature is not valid;

3) Associating the integer i with the point P;

4) Calculating the integer f=c-i modulo r;

5) Concatenating the t least significant bytes of d with the message m' obtained from f by removing the a least significant bytes;

6) For b ranging from 0 to 2^{8k}-1, repeating the following step:

6a) Concatenating the message m' with b in order to obtain m and calculating h=H(m); verifying that the a most significant bytes of h and the a least significant bytes of f are identical; if yes, the signature of the message m is valid and the method is terminated;

7) Otherwise the signature is not valid.

17. (Amended) A method for generating and verifying an electronic signature according to claim 1, wherein the operations are effected on an elliptic curve forming a group structure and having at least one point G, which is the generator of a sub-group of order r.

18. (Amended) A method for generating and verifying an electronic signature according to claim 1, wherein the operations are effected in the multiplicative group of the integers modulo a prime number p.

19. (Amended) A method for generating and verifying an electronic signature according to claim 1, wherein the operations are effected in a multiplicative sub-group of order r of the multiplicative group of the integers modulo a prime number p with r dividing p-1.

20. (Amended) An electronic device that executes the method of claim 1, wherein said device is a portable device.

21. (Amended) An electronic device that executes the method of claim 1, wherein the device is a smart card.

22. (Amended) An electronic device that executes the method of claim 1, wherein the device is a contactless card.

23. (Amended) An electronic device that executes the method of claim 1, wherein the device is a PCMCIA card.

24. (Amended) An electronic device that executes the method of claim 1, wherein the device is a badge.

25. (Amended) An electronic device that executes the method of claim 1, wherein the device is an intelligent watch.

Add the following new claims:

26. (New) A method according to claim 10 for preprocessing the calculations making it possible to increase performance, comprising the further step of putting in memory in a table the pairs of integers (u,i) so that these integers are accessible to the value of i modulo 2^{8t}, t being an integer parameter.

27. (New) A method according to claim 2 for modifying the signature scheme with partial reconstruction of the message comprising the further step of replacing the signature (c,d) with the signature (h_2,d) with $h_2=c*d^{-1}$ modulo r.

28. (New) A method for generating and verifying an electronic signature according to claim 2, wherein the operations are effected on an elliptic curve forming a group structure and having at least one point G, which is the generator of a sub-group of order r.

29. (New) A method for generating and verifying an electronic signature according to claim 2, wherein the operations are effected in the multiplicative group of the integers modulo a prime number p.

30. (New) A method for generating and verifying an electronic signature according to claim 2, wherein the operations are effected in a multiplicative sub-group of order r of the multiplicative group of the integers modulo a prime number p with r dividing p-1.

REMARKS

Entry of the foregoing amendment is respectfully requested. This amendment is intended to place the claims in a more conventional format and eliminate the multiple dependency of the claims.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By: James LaBarre
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

Date: January 30, 2002

Attachment to Preliminary Amendment dated January 30, 2002

Marked-up Claims 1-25

1. (Amended) An electronic signature method comprising a generation method and a verification method allowing total reconstitution of [the] a message, [the] said method utilising a redundancy function R, a set having a group structure of order r, where r is a prime number [r], with a zero element denoted O and generating the point G, [the] and employing a private key [being] that is a positive integer less than r, [the] and a public key being the point W=s.G, [the] said method using a non-zero integer constant k, [characterised in that] wherein the signature generation method includes the following four steps:

1) Generating a random number u between 1 and r-1 and calculating V=u.G;

2) Associating an integer i with the point V and calculating c=i+f modulo r; if c=0, returning to step 1[)];

3) Calculating the integer $d=u^{-1}*(k+s*c)$ modulo r; if d=0, returning to step 1[)]; and

4) [The signature is] Utilizing the pair of integers (c,d) as the signature;

and [in that] wherein the signature verification method includes the following six steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [1,r-1], the signature is not valid;

2) Calculating the integers $h = d^{-1}$ modulo r, $h_1=k*h$ modulo r and $h_2=c*h$ modulo r;

3) Calculating the point $P = h_1G + h_2W$; if P=0, the signature is not valid;

Attachment to Preliminary Amendment dated January 30, 2002

Marked-up Claims 1-25

4) Associating an integer i with the point P;

5) Calculating the integer f=c-i modulo r; and

6) Finding the message m from f and verifying that f=R(m); if yes, the signature of the message m is valid; otherwise the signature is not valid.

2. (Amended) An electronic signature method comprising a generation method and a signature verification method allowing partial reconstruction of [the] a message, the message m to be signed being divided into two parts, the first part m_1 of constant size being reconstituted from the signature, the second part m_2 being transmitted with the signature of the method, [the] said method utilising a redundancy function R, a set having a group structure of order r, where r is a prime number [r], with a zero element denoted O and generating the point G, [the] and employing a private key [being] that is a positive integer less than r and [the] a public key being the point W=s.G, [characterised in that] wherein the method of generating the signature of a message m consisting of the messages m_1 and m_2 includes the following six steps:

1) Generating a random integer u between 1 and r-1 and calculating V=u.G;

2) Calculating $f_1=R(m_1)$;

3) Associating an integer i with the point V and calculating $c=i+f_1$ modulo r; if c=0, returning to step 1;

4) Calculating $f_2=H(m_2)$, where H is a hash function;

Attachment to Preliminary Amendment dated January 30, 2002

Marked-up Claims 1-25

5) Calculating the integer $d=u^{-1}*(f_2+s*c)$ modulo r; if d=0, returning to step 1; and

6) [The signature is] Utilizing the pair of integers (c,d) as the signature;

and [in that] wherein the signature verification method takes as an input a pair of integers (c,d) and the partial message m_2 and comprises the following seven steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [1,r-1], the signature is not valid;

2) Calculating $f_2=H(m_2)$, where H is a hash function;

3) Calculating the integers $h=d^{-1}$ modulo r, $h_1=f_2*h$ modulo r and $h_2=c*h$ modulo r;

4) Calculating the point $P=h_1G+h_2W$; if P=0, the signature is not valid;

5) Associating the integer i with the point P;

6) Calculating the integer $f_1=c-i$ modulo r; and

7) Obtaining the message m_1 from f_1 and verifying that $f_1=R(m_1)$; if yes, the signature of the message m is valid; otherwise the signature is not valid.

3. (Amended) An electronic signature method comprising a generation method and a signature verification method [characterised in that it consists in] that comprises including part of the message inside the signature by suitably choosing the random data used during the generation of the signature.

Attachment to Preliminary Amendment dated January 30, 2002

Marked-up Claims 1-25

4. (Amended) An electronic signature method comprising a generation method and a signature verification method[, characterised in that it consists in] that comprises the steps of eliminating some of the bytes representing the signature, [the complete reconstitution of] and reconstituting the signature [taking place] during the verification phase.

5. (Amended) A method according to claim 3 for improving the Nyberg-Rueppel signature scheme [according to Claim 3], comprising a generation method and a verification method [and consisting in including] in which part of the message of size t bytes is included in the integer d, t being a small integer, the signature being [the] a pair of integers (c,d), the t least significant bytes of [the] an integer g containing t bytes of the message, the said method using a redundancy function R, a set having a group structure of order r, where r is a prime number [r], with a zero element denoted O and generating the point G, [the] and employing a private key [being] that is a positive integer s less than r and [the] a public key being the point W=s.G, [characterised in that] wherein the method of generating the signature of a message m includes the following five steps:

1) Removing the t least significant bytes of the message m and storing the result in m'; calculating f=R(m');

2) Generating a random number u between 1 and r-1 and calculating V=u.G;

Attachment to Preliminary Amendment dated January 30, 2002

Marked-up Claims 1-25

3) Associating an integer i with the point V and calculating c=i+f modulo r; returning to step 1[)] if c=0.

4) Calculating the integer d=u-s*c modulo r; if d is not equal to m modulo 2^{8t}, returning to step 2[)]; and

5) [The signature is] Utilizing the pair of integers (c,d) as the signature; and [in that] wherein the signature verification method includes the following five steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [0,r-1], the signature is not valid;

2) Calculating the point P=d.G+c.W; if P=0, the signature is not valid;

3) Associating the integer i with the point P;

4) Calculating the integer f=c-i modulo r;

5) Obtaining the message m' from f and verifying that f=R(m'); if such is not the case, the signature is not valid; if such is the case, the signature is valid and the message m is the concatenation with the message m' of the t least significant bytes of the integer d.

6. (Amended) A method according to claim 5 for the preprocessing of the signature generation [according to Claim 5, making it possible] to accelerate the generation of the signatures, [the] said method comprising a pretreatment phase and a signature generation phase, [the] said pretreatment phase taking as an input [the] a secret key s and

[consisting in] putting in memory in a table a large number of values (i, x_u) with x_u=u-s*i modulo r and i being the integer associated with the point V=u.G, so that these values can be accessed by the remainder of x_u modulo 2^{8t}, [the] said signature generation phase utilising a redundancy function R, a set having a group structure of order r, where r is a prime number [r], with a zero element denoted O and generating the point G, [the] and employing a private key [being] that is a positive integer s less than r and [the] a public key being the point W=s.G, [the] said signature generation phase [being characterised by] comprising the following eight steps:

1) Removing the t least significant bytes in the message m and storing the result in the message m'; calculating f=R(m'). The t least significant bytes of the message m are stored in the integer d;

2) Calculating the integer y=s*f modulo r and the integer 1=y modulo 2^{8t};

3) If y<r/2, first of all executing step 4 and next step 5; otherwise executing first of all step 5 and next step 4;

4) Accessing the elements of the table where the remainder modulo 2^{8t} is 1+d modulo 2^{8t} and selecting an element such that x_u is greater than or equal to y; if such an element exists, it is eliminated from the table and the method passes to step 6[)];

5) Accessing the elements of the table where the remainder modulo 2^{8t} is 1+d+r modulo 2^{8t} and selecting an element such that x_u is less than y; if such an element exists, it is eliminated from the table and the method passes to step 6[)];

6) Calculating the integer $d=x_u$-y modulo r;

7) Obtaining the integer i associated with x_u and calculating c=i+f modulo r; and

8) [The signature is] Utilizing the pair of integers (c,d) as the signature.

7. (Amended) A method according to claim 2 for improving the signature scheme with partial reconstitution of the message [according to Claim 2], [the] said method comprising a signature generation method and a signature verification method, [the] said method [consisting in] including part of the message of size t bytes in the integer d [defined previously], t being a small integer, the t least significant bytes of the integer d containing t bytes of the message, [the] said method utilising a redundancy function R, a set having a group structure of order r, where r is a prime number [r], with a zero element denoted O and generating a point G, [the] and employing a private key [being] that is a positive integer less than r and [the] a public key being the point W=s.G, [characterised in that] wherein the method of generating the signature of a message m consisting of the messages m_1 and m_2 includes the following six steps:

1) Generating a random integer u between 1 and r-1 and calculating V=u.G;

2) Calculating $f_1=R(m_1)$;

3) Associating an integer i with the point V and calculating $c=i+f_1$ modulo r; if c=0, returning to step 1;

Attachment to Preliminary Amendment dated January 30, 2002

Marked-up Claims 1-25

4) Calculating $f_2=H(m_2)$, where H is a hash function;

5) Calculating the integer $d=u^{-1}*(f_2+s*c)$ modulo r; if $d=0$ or if d is not equal to m_2 modulo 2^{8t}, returning to step 1; and

6) [The signature is] Utilizing the pair of integers (c,d) as the signature, and the message to be transmitted is m'_2 consisting of m_2 deprived of its t least significant bytes; and [in that] wherein the signature verification method takes as an input a pair of integers (c,d) and the partial message m'_2 and comprises the following eight steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [1,r-1], the signature is not valid;

2) Making up m'_2 as m_2 by adding to it the t least significant bytes of d;

3) Calculating $f_2=H(m_2)$, where H is a hash function;

4) Calculating the integers $h=d^{-1}$ modulo r, $h_1=f_2*h$ modulo r and $h_2=c*h$ modulo r;

5) Calculating the point $P=h_1G+h_2W$; if $P=0$ the signature is not valid;

6) Associating the integer i with the point P;

7) Calculating the integer $f_1=c\text{-}i$ modulo r; and

8) Obtaining the message m_1 from $f_1$and verifying that $f_1=R(m_1)$; if yes, the signature of the message m is valid; otherwise the signature is not valid.

Attachment to Preliminary Amendment dated January 30, 2002

Marked-up Claims 1-25

8. (Amended) A method [consisting in] that includes removing t bytes from [the] a chain of bytes representing [the] an integer d [when the] from a signature that is the pair of integers (c,d), [the] said method comprising a signature generation method and a signature verification method, [the] said method being applied to the Nyberg and Rueppel signature scheme, [characterised in that] wherein the [modified] signature generation method includes the following two steps:

1) Generating the signature of the message m using the Nyberg and Rueppel signature scheme, to obtain the pair of integers (c,d); and

2) Calculating d', the integer quotient of the division of the integer d by 2^{8t}; [the signature is] and utilizing the pair of integers (c,d') as the signature;

and [in that the modified] wherein the signature verification method takes as an input a pair (c,d') and includes the following five steps:

1) If c does not belong to the interval [1,r-1], the signature is not valid;

2) Calculating the point $P=d'*2^{8t}.G+c.W$;

3) For j ranging from 0 to 2^{8t}-1, executing the following steps:

3[)]a) If P=O, executing step 3[)]d);

3[)]b) Associating the integer i with the point P and calculating the integer f=c-i modulo r;

3[)]c) Finding the message m from f and verifying that f=R(m); if yes, executing step 5[)];

3[)]d) Replacing P with P+G;

4) The signature is not valid and the method is terminated;

5) If the integer $d=d'*2^{8t}+j$ does not belong to the interval [0,r-1], the signature is not valid; otherwise the signature is valid and the method is terminated.

9. (Amended) A method [consisting in] that includes removing t bytes from [the] a chain of bytes representing [the] an integer d [when the] from a signature that is the pair of integers (c,d), [the] said method comprising a signature generation method and a signature verification method, [the said method to the signature diagram] with partial reconstitution of [the] a message according to Claim 2, [characterised in that the modified] wherein the signature generation method includes the following two steps:

1) Generating the signature of [the] a message m using the signature scheme with partial reconstruction of the message [previously described] according to claim 2, in order to obtain the pair of integers (c,d); and

2) Calculating d', the integer quotient of the division of the integer d by 2^{8t}; wherein the signature is the pair of integers (c,d');

and [in that] wherein the modified signature verification method takes as an input a pair (c,d') and a message m_2 and includes the following two steps:

1) For i ranging from 0 to 2^{8t}-1, calculating the integer $d=d'*2^{8t}+i$ and executing the signature verification method with partial reconstitution of the message

Attachment to Preliminary Amendment dated January 30, 2002

Marked-up Claims 1-25

[previously described] according to claim 2, the signature to be verified being (c,d); if the signature verification method recognises the signature (c,d) as valid, the signature is valid, and the method is terminated;

2) Otherwise the [The] signature is not valid.

10. (Amended) A method for improving the Nyberg and Rueppel scheme making it possible to increase the size of the messages to be signed by t bytes, t being an integer variable, [the] said method comprising a signature generation method and a signature verification method, [the] said method utilising a redundancy function R, a set having a group structure of order r, where r is a prime number [r], with a zero element denoted O and generating the point G, [the] and employing a private key [being] that is a positive integer s less than r and [the] a public key being the point W=s.G, [characterised in that] wherein the method of generating the signature of a message m includes the following five steps:

1) Generating a random number u and calculating V=u.G;

2) Obtaining the message m' by removing from the message m the t least significant bytes and calculating f=R(m');

3) Associating an integer i with the point V and calculating c=i+f modulo r; returning to step 1[)] if c=0 and if i is not equal to m modulo 2^{8t};

4) Calculating d=u-s*c modulo r; and

Attachment to Preliminary Amendment dated January 30, 2002

Marked-up Claims 1-25

5) [The signature is] Utilizing the pair of integers (c,d) as the signature; and [in that] wherein the signature verification method includes the following four steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [0,r-1], the signature is not valid;

2) Calculating the point P=d.G+c.W; if P=O, the signature is not valid;

3) Associating the integer i with the point P and calculating the integer f=c-i modulo r; and

4) Finding the message m' from f and verifying that f=R(m'); if yes, finding the message m by concatenating the t least significant bytes of i with the message m'. The signature of the message m is then valid; otherwise the signature is not valid.

11. (Amended) A method for improving [the] a signature scheme with partial reconstitution of the message according to Claim 2, [the] said method comprising a signature generation method and a signature verification method, [the said method] and making it possible to increase by t bytes the size of the message m_1 reconstituted from the signature, t being an integer variable, said method utilising a redundancy function R, a set having a group structure of order r, where r is a prime number [r], with a zero element denoted O and generating the point G, [the] and employing a private key [being] that is a positive integer less than r and [the] a public key being the point W=s.G, [characterised in

Attachment to Preliminary Amendment dated January 30, 2002

Marked-up Claims 1-25

that] wherein the method of generating the signature of a message m includes the following six steps:

1) Generating a random integer u between 1 and r-1 and calculating $V=u.G$;

2) Obtaining m'_1 by removing the t least significant bytes from the message m_1. Calculating $f_1=R(m'_1)$;

3) Associating an integer i with the point V and calculating $c=i+f_1$ modulo r; if $c=0$ or if i is not equal to m_1 modulo 2^{8t}, returning to step 1;

4) Calculating $f_2=H(m_2)$, where H is a hash function;

5) Calculating the integer $d=u^{-1}*(f_2+s*c)$ modulo r; if $d=0$, returning to step 1; and

6) [The signature is] Utilizing the pair of integers (c,d) as the signature;

and [in that] wherein the signature verification method takes as an input a pair of integers (c,d) and the partial message m_2 and comprises the following seven steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [1,r-1], the signature is not valid;

2) Calculating $f_2=H(m_2)$, where H is a hash function;

3) Calculating the integers $h=d^{-1}$ modulo r, $h_1=f_2*h$ modulo r and $h_2=c*h$ modulo r;

4) Calculating the point $P=h_1G+h_2W$; if $P=O$, this signature is not valid.

5) Associating the integer i with the point P;

Attachment to Preliminary Amendment dated January 30, 2002

Marked-up Claims 1-25

6) Calculating the integer $f_1 = c-i$ modulo r; and

7) Obtaining the message m'_1 from f_1 and verifying that $f_1 = R(m'_1)$; if yes, obtaining m_1 by concatenating the t least significant bytes of the integer i with the message m'_1. The signature of the message m is then valid; otherwise the signature is not valid.

12. (Amended) A method according to claim 11 for preprocessing the calculations making it possible to increase [the performances of the methods according to Claims 10 and 11, characterised in that it consists in] performance, comprising the further step of putting in memory in a table the pairs of integers (u,i) [as defined previously] so that these integers are accessible to the value of i modulo 2^{8t}, t being an integer parameter.

13. (Amended) A method for improving the Nyberg and Rueppel signature scheme consisting in removing t bytes from [the] an integer c, t being an integer variable, [the] said method comprising a signature generation method and a signature verification method, the signature consisting of the pair of integers (c,d), [characterised in that] wherein the signature generation method includes the following two steps:

1) Generating the signature of [the] a message m using the Nyberg-Rueppel signature scheme in order to obtain the pair of integers (c,d); and

2) Calculating c', the integer quotient of the division of the integer c by 2^{8t}, and employing[. The signature is] the pair of integers (c',d) as the signature;

Attachment to Preliminary Amendment dated January 30, 2002

Marked-up Claims 1-25

and [in that] wherein the signature verification method takes as an input the pair of integers (c',d) and includes the following five steps:

1) If d does not belong to the interval [0,r-1], the signature is not valid;

2) Calculating the point P=d.G+c'*2^{8t}.W;

3) For j ranging from 0 to 2^{8t}-1, executing the following steps:

3[)]a) If P=O, executing step 3[)]d);

3[)]b) Associating the integer i with the point P and calculating the integer f=c-i modulo r;

3[)]c) Finding the message m from f and verifying that f=R(m); if yes, executing step 5[)];

3[)]d) Replacing P by P+W;

4) The signature is not valid and the method is terminated;

5) If the integer c=c'*2^{8t}+j does not belong to the interval [1,r-1], the signature is not valid; otherwise the signature is valid and the method is terminated.

14. (Amended) A method according to claim 2 for improving the signature scheme with partial reconstitution of the message [according to Claim 2, consisting in] that includes the further step of removing t bytes from the integer c [defined according to Claim 2], t being an integer variable, [the] said method comprising a signature generation method

Attachment to Preliminary Amendment dated January 30, 2002

Marked-up Claims 1-25

and a signature verification method, [characterised in that] wherein the signature generation method comprises the following two steps:

1) Generating the signature of the message m, using the signature scheme with partial reconstitution of the message in order to obtain the pair of integers (c,d); and

2) Calculating c', the integer quotient of the division of the integer c by 2^{8t}; [the signature is] and utilizing the pair of integers (c',d) as the signature;

and [in that] wherein the signature verification method takes as an input a pair of integers (c',d) and a message m_2 and comprises the following eight steps:

1) If d does not belong to the interval [1,r-1], the signature is not valid;

2) Calculating $f_2=H(m_2)$, where H is a hash function;

3) Calculating the integers $h=d^{-1}$ modulo r, $h_1=f_2*h$ modulo r and $h_2=c'*2^{8t}*h$ modulo r;

4) Calculating the point $P=h_1.G+h_2.W$;

5) Calculating the point $Z=h.W$;

6) For j ranging from 0 to 2^{8t}-1, executing the following steps:

6[)]a) If P=O, executing step 6[)]d);

6[)]b) Associating the integer i with the point P and calculating the integer $f_1=c-i$ modulo r;

6[)]c) Finding the message m_1 from f_1 and verifying that $f_1=R(m_1)$; if yes, executing step 8[)];

Attachment to Preliminary Amendment dated January 30, 2002

Marked-up Claims 1-25

6[)]d) Replacing P with P+Z;

7) The signature is not valid and the method is terminated;

8) If the integer $c=c'*2^{8t}+j$ does not belong to the interval [1,r-1], the signature is not valid; otherwise the signature is valid and the method is terminated.

15. (Amended) A method according to claim 1 for modifying the signature scheme with partial reconstruction of the message [according to any one of the preceding claims, characterised in that it consists in] comprising the further step of replacing the signature (c,d) with the signature (h_2,d) with $h_2=c*d^{-1}$ modulo r.

16. (Amended) A method for improving the Nyberg-Rueppel signature scheme, said method comprising a signature generation method and a signature verification method, the said method [consisting in] having the step of including part of [the] a message of size t bytes in [the] an integer d, the signature being the pair of integers (c,d), t being a small integer, the t least significant bytes of the integer d containing t bytes of the message, [the] said method utilising a set having a group structure of order r, where r is a prime number [r], with a zero element denoted O and generating the point G, [the] and employing a private key [being] that is a positive integer s less than r and [the] a public key being the point W=s.G, [characterised in that] wherein the method of generating the signature of a message m using the integer parameters t, a and k includes the following seven steps:

Attachment to Preliminary Amendment dated January 30, 2002

Marked-up Claims 1-25

1) Calculating h=H(m), H being a hash function;

2) Removing the t least significant bytes and the k most significant bytes of the message m and storing the result in m';

3) Storing [in] as f the result of the concatenation with m' of the a most significant bytes of h;

4) Generating a random number u between 1 and r-1 and calculating V=u.G;

5) Associating an integer i with the point V and calculating c=i+f modulo r; returning to step 4[)] if c=0;

6) Calculating the integer d=u-s*c modulo r; if d is not equal to m modulo 2^{8t} returning to step 4[)]; and

7) [The signature is] Utilizing the pair of integers (c,d) as the signature;

and [in that] wherein the signature verification method includes the following seven steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [0,r-1], the signature is not valid;

2) Calculating the point P=d.G+c.W; if P=O, the signature is not valid;

3) Associating the integer i with the point P;

4) Calculating the integer f=c-i modulo r;

5) Concatenating the t least significant bytes of d with the message m' obtained from f by removing the a least significant bytes;

6) For b ranging from 0 to 2^{8k}-1, repeating the following step:

Attachment to Preliminary Amendment dated January 30, 2002

Marked-up Claims 1-25

6[)]a) Concatenating the message m' with b in order to obtain m and calculating h=H(m); verifying that the a most significant bytes of h and the a least significant bytes of f are identical; if yes, the signature of the message m is valid and the method is terminated;

7) Otherwise the [The] signature is not valid.

17. (Amended) A method for generating and verifying an electronic signature according to [any one of the preceding claims, characterised in that] claim 1, wherein the operations are effected on an elliptic curve forming a group structure and having at least one point G, which is the generator of a sub-group of order [a prime number] r.

18. (Amended) A method for generating and verifying an electronic signature according to [any one of the preceding claims, characterised in that] claim 1, wherein the operations are effected in the multiplicative group of the integers modulo a prime number p.

19. (Amended) A method for generating and verifying an electronic signature according to [any one of the preceding claims, characterised in that] claim 1, wherein the operations are effected in a multiplicative sub-group of order [a prime number] r of the multiplicative group of the integers modulo a prime number p with r dividing p-1.

Attachment to Preliminary Amendment dated January 30, 2002

Marked-up Claims 1-25

20. (Amended) An electronic device [according to any one of the preceding claims, characterised in that the device performing the test] that executes the method of claim 1, wherein said device is a portable device.

21. (Amended) An electronic device [according to any one of the preceding claims, characterised in] that executes the method of claim 1, wherein the device is a smart card.

22. (Amended) An electronic device [according to any one of the preceding claims, characterised in] that executes the method of claim 1, wherein the device is a contactless card.

23. (Amended) An electronic device [according to any one of the preceding claims, characterised in] that executes the method of claim 1, wherein the device is a PCMCIA card.

24. (Amended) An electronic device [according to any one of the preceding claims, characterised in] that executes the method of claim 1, wherein the device is a badge.

Attachment to Preliminary Amendment dated January 30, 2002

Marked-up Claims 1-25

25. (Amended) An electronic device [according to any one of the preceding claims, characterised in] that executes the method of claim 1, wherein the device is an intelligent watch.

SIGNATURE SCHEMES BASED ON THE DISCRETE LOGARITHM WITH PARTIAL OR TOTAL RECONSTITUTION OF THE MESSAGE

The invention consists of two novel electronic signature schemes based on the discrete logarithm problem, the first allowing the total reconstitution of the message, the second allowing the partial reconstitution of the message, as well as two techniques for reducing the size of the electronic signatures.

An electronic signature of a message is a number depending both on a secret key known only to the person signing the message, and the content of the message to be signed. An electronic signal must be verifiable: it must be possible for a third person to verify the validity of the signature, without knowledge of the secret key of the person signing the message being required.

There exist two types of electronic signature scheme:

- Electronic signature schemes requiring the original message for verification of the signature.
- Electronic signature schemes with reconstitution of the message. The original message is obtained after the signature itself. Since the original message is not necessary for verifying the signature, the total size of the signature is shorter.

There are many electronic signature methods. The best known are:

- RSA signature scheme: this is the most widely used electronic signature scheme. Its security is based on the difficulty of factorising large numbers;
- Rabin signature scheme. Its security is also based on the difficulty of factorising large numbers;
- Signature scheme of the El-Gamal type. Its security is based on the difficulty of the discrete logarithm problem. The discrete logarithm problem consists in determining, if such exists, an integer x such that $y=g^x$ with y and g two elements of a set E having a group structure;
- Schnorr signature scheme. This is a variant of the signature scheme of the El-Gamal type.

There exists another variant of the signature scheme of the El-Gamal type allowing the total reconstruction of the message, called the Nyberg and Rueppel signature scheme. This scheme is described in the article "A new signature scheme based on the DSA, giving message recovery" which appeared in "Proceedings of the first ACM conference on communications and computer security, 1993, 58-61". A variant scheme based on the elliptic curve is described in the document "IEEE P1363 draft. Standard specifications for public key cryptography. August 1998." This variant uses a redundancy function R, an elliptic curve forming a group structure whose zero element is denoted O and a point G on the curve, which point G is the generator of a sub-group of order a prime number r. The private key is a positive integer s smaller than r and the public key is the point W=s.G, the notation s.G designating the sum, in the sense of the addition of the elliptic curve, of s points taken to be equal to G. The method of generating the signature of a message m includes the following five steps:

1) Generating a random number u between 0 and r-1 and calculating V=u.G;

2) Calculating the integer f=R(m);

3) Associating with the point V an integer i and calculating c=i+f modulo r; returning to step 1) if c=0;

4) Calculating d=u-s*c modulo r;

5) The signature is the pair of integers (c,d).

The method of verifying the signature includes the following four steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [0,r-1], the signature is not valid;

2) Calculating the point P=d.G+c.W; if P=0, the signature is not valid;

3) Associating the integer i with the point P and calculating the integer $f=c-i$ modulo r;

4) Finding the message m from f and verifying that $f=R(m)$; if yes, the signature of the message m is valid; otherwise this signature is not valid.

The first method of the invention consists of another variant of a signature scheme of the El-Gamal type. This variant allows the total reconstitution of the message. The variant is described in the context of the use of elliptic curves. It is however possible to use this variant in any set having a group structure for which the discrete logarithm problem is difficult, for example the multiplicative group of the integers modulo a prime number or the multiplicative sub-group of order a large prime number r of the integers modulo a prime number p with r dividing p-1. This variant uses a redundancy function R, an elliptic curve forming a group structure whose zero element is denoted O and a point G on the curve, which point G is the generator of a sub-group of order a prime number r. The private key is a positive integer s less than r and the public key is the point $W=s.G$. This variant uses a non-zero integer constant k. The method of generating the signature includes the following four steps:

1) Generating a random number u between 1 and r-1 and calculating $V=u.G$;

2) Associating an integer i with the point V and calculating $c=i+f$ modulo r; if $c=0$, returning to step 1);

3) Calculating the integer $d=u^{-1}*(k+s*c)$ modulo r; if d=0, returning to step 1);

4) The signature is the pair of integers (c,d).

The corresponding method of verifying the signature includes the following six steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [1,r-1], the signature is not valid;

2) Calculating the integers $h = d^{-1}$ modulo r, $h_1=k*h$ modulo r and $h_2=c*h$ modulo r;

3) Calculating the point $P = h_1G + h_2W$; if P=0, the signature is not valid;

4) Associating an integer i with the point P;

5) Calculating the integer f=c-i modulo r;

6) Finding the message m from f and verifying that f=R(m); if yes, the signature of the message m is valid; otherwise the signature is valid.

The previously described method therefore makes it possible to obtain an electronic signature scheme whose security is based on the difficulty of the discrete logarithm problem and allowing total reconstitution of the message.

The invention also comprises a second electronic signature method allowing partial reconstruction of the message. The previously described signature scheme allows total reconstitution of the message. However, the total size of the message to be signed is limited by the size of the arguments of the redundancy function R. The second method of the invention makes it possible to sign a message of any size. The message m to be signed is divided into two parts: the first part m_1 of constant size is reconstituted from the signature, the second part m_2 is transmitted with the signature of the message. The total size of the signature and of the message to be transmitted is therefore reduced by the size of the part m_1. The signature scheme is described in the context of the use of elliptic curves. It is however possible to use this scheme in any set having a group structure for which the discrete logarithm problem is difficult, for example the multiplicative group of integers modulo a prime number or the multiplicative sub-group of order a large prime number r of the integers modulo a prime number p with r dividing $p-1$. The signature scheme utilises a redundancy function r, an elliptic curve forming a group structure in which the element zero is denoted O and a point G on the curve, which point G is the generator of a sub-group of order a prime number r. The private key is a positive integer s less than r and the public key is the point $W=s.G$. The method of generating the signature of a message m consisting of the messages m_1 and m_2 includes the following six steps:

1) Generating a random integer u between 1 and $r-1$ and calculating $V=u.G$;

2) Calculating $f_1=R(m_1)$;

3) Associating an integer i with the point V and calculating $c=i+f_1$ modulo r; if $c=0$, returning to step 1;

4) Calculating $f_2=H(m_2)$, where H is a hash function;

5) Calculating the integer $d=u^{-1}*(f_2+s*c)$ modulo r; if d=0, returning to step 1;

6) The signature is the pair of integers (c,d).

The method for verifying the signature takes as an input a pair of integers (c,d) and the partial message m_2 and comprises the following seven steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [1,r-1], the signature is not valid;

2) Calculating $f_2=H(m_2)$, where H is a hash function;

3) Calculating the integers $h=d^{-1}$ modulo r, $h_1=f_2*h$ modulo r and $h_2=c*h$ modulo r;

4) Calculating the point $P=h_1G+h_2W$; if P=0, the signature is not valid;

5) Associating the integer i with the point P;

6) Calculating the integer $f_1=c-i$ modulo r;

7) Obtaining the message m_1 from f_1 and verifying that $f_1=R(m_1)$; if yes, the signature of the message m is valid; otherwise the signature is not valid.

The previously described method therefore makes it possible to obtain an electronic signature scheme whose security is based on the difficulty of the discrete logarithm and allowing partial reconstruction of the message. The advantage of such a scheme is to reduce the total size of the signature and of the message to be transmitted without however imposing a size constraint on this message.

The invention also consists of two general techniques for minimising the total size of the signature and of the message to be transmitted. The first technique consists in including part of the message inside the signature whilst suitably choosing the random data used during the generation of the signature. The second technique consists in eliminating some of the bytes representing the signature, the complete reconstitution of the signature taking place during the verification phase.

The third method of the invention consists of an improvement to the Nyberg-Rueppel signature scheme mentioned previously, and consists in including part of the message of size t bytes in the integer d defined previously, t being a small integer. In this method, the t least significant bytes of the integer g contain t bytes of the message. The third method of the invention therefore makes it possible to increase the size of the message to be signed by t bytes compared with the Nyberg-Rueppel signature scheme described previously. The third method uses a redundancy function R, an elliptic curve forming a group structure in which the zero element is denoted O and a point G on the curve, which point G is the generator of a sub-group of order a prime number r. The private key is a positive integer s less than r and the public key is the point W=s.G. The method of generating the signature of a message m includes the following five steps:

1) Removing the t least significant bytes of the message m and storing the result in m’; calculating f=R(m’);

2) Generating a random number u between 1 and r-1 and calculating V=u.G;

3) Associating an integer i with the point V and calculating c=i+f modulo r; returning to step 1) if c=0.

4) Calculating the integer d=u-s*c modulo r; if d is not equal to m modulo 2^{8t}, returning to step 2);

5) The signature is the pair of integers (c,d).

The method for verifying the signature includes the following five steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [0,r-1], the signature is not valid;

2) Calculating the point P=d.G+c.W; if P=0, the signature is not valid;

3) Associating the integer i with the point P;

4) Calculating the integer f=c-i modulo r;

5) Obtaining the message m' from f and verifying that f=R(m'); if such is not the case, the signature is not valid; if such is the case, the signature is valid and the message m is the concatenation to the message m' of the t least significant bytes of the integer d.

It is possible to effect a preprocessing of the data making it possible to accelerate the generation of the signature according to the signature scheme described previously. The pretreatment method takes as an input the secret key s and consists in putting in memory in a table a large number of values (i, x_u) with x_u=u-s*i modulo r and i being the integer associated with the point V=u.G, so that the values can be accessed by the remainder of x_u modulo 2^{8t}. The signature generation method with pretreatment of the data uses a redundancy function R, an elliptic curve forming a group structure in which the zero element is denoted O and a point G on the curve, which point G is the generator of a sub-group of order a prime number r. The private key is a positive integer s less than r and the public key is the point W=s.G.

The signature generation method with preprocessing of the data includes the following eight steps:

1) Removing the t least significant bytes in the message m and storing the result in the message m'; calculating f=R(m'). The t least significant bytes of the message m are stored in the integer δ;

2) Calculating the integer y=s*f modulo r and the integer λ=y modulo 2^{8t};

3) If y<r/2, first of all executing step 4 and next step 5; otherwise executing first of all step 5 and next step 4;

4) Accessing the elements of the table where the remainder modulo 2^{8t} is $\lambda+\delta$ modulo 2^{8t} and selecting an element such that x_u is greater than or equal to y; if such an element exists, it is eliminated from the table and the method passes to step 6);

5) Accessing the elements of the table where the remainder modulo 2^{8t} is $\lambda+\delta+r$ modulo 2^{8t} and selecting an element such that x_u is less than y; if such an element exists, it is eliminated from the table and the method passes to step 6);

6) Calculating the integer $d=x_u-y$ modulo r;

7) Obtaining the integer i associated with x_u and calculating $c=i+f$ modulo r;

8) The signature is the pair of integers (c,d).

The fourth method of the invention consists of an improvement to the signature scheme based on the discrete logarithm with partial reconstitution of the message described previously. The fourth method of the invention consists in including part of the message of size t bytes in the integer d defined previously, t being a small integer. In this method, the t least significant bytes of the integer d contain t bytes of the message. The fourth method of the invention therefore makes it possible to reduce by t bytes the total size of the signature and of the message to be transmitted. The signature scheme uses a redundancy function R, an elliptic curve forming a group structure in which the zero element is denoted O and a point G on the curve, which point G is the generator of a sub-group of order a prime number r. The private key is a positive integer s less than r and the public key is the point W=s.G. The method of generating the signature of a message m consisting of the messages m_1 and m_2 includes the following six steps:

1) Generating a random integer u between 1 and r-1 and calculating V=u.G;

2) Calculating $f_1=R(m_1)$;

3) Associating an integer i with the point V and calculating $c=i+f_1$ modulo r; if c=0, returning to step 1;

4) Calculating $f_2=H(m_2)$, where H is a hash function;

5) Calculating the integer $d=u^{-1}*(f_2+s*c)$ modulo r; if d=0 or if d is not equal to m_2 modulo 2^{8t}, returning to step 1;

6) The signature is the pair of integers (c,d) and the message to be transmitted is m'_2 consisting of m_2 deprived of its t least significant bytes.

The signature verification method takes as an input a pair of integers (c,d) and the partial message m'_2 and comprises the following eight steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [1,r-1], the signature is not valid;

2) Making up m'_2 as m_2 by adding to it the t least significant bytes of d;

3) Calculating $f_2=H(m_2)$, where H is a hash function;

4) Calculating the integers $h=d^{-1}$ modulo r, $h_1=f_2*h$ modulo r and $h_2=c*h$ modulo r;

5) Calculating the point $P=h_1G+h_2W$; if P=0 the signature is not valid;

6) Associating the integer i with the point P;

7) Calculating the integer $f_1=c-i$ modulo r;

8) Obtaining the message m_1 from f_1 and verifying that $f_1=R(m_1)$; if yes, the signature of the message m is valid; otherwise the signature is not valid.

The fifth method of the invention consists in eliminating t bytes from the chain of bytes representing the integer d when the signature is the pair of integers (c,d). This method applies to the Nyberg and Rueppel signature scheme and to the signature scheme with partial reconstruction of the message described previously. The modified signature generation method includes the following two steps:

1) Generating the signature of the message m using the Nyberg and Rueppel signature scheme or the signature scheme with partial reconstruction of the message described previously, in order to obtain the pair of integers (c,d);

2) Calculating d', the integer quotient of the division of the integer d by 2^{8t}. The signature is the pair of integers (c,d').

The modified signature verification method takes as an input a pair (c,d') and a message m_2 and includes the following two steps in the case of the signature scheme with partial reconstitution of the message described previously:

1) For i ranging from 0 to 2^{8t}-1, calculating the integer $d=d'*2^{8t}+i$ and executing the signature verification method with partial reconstitution of the message described previously, the signature to be verified being (c,d); if the signature verification method recognises the signature (c,d) as valid, the signature is valid and the method is terminated;

2) If step 1) has not succeeded, the signature is not valid.

In the case of the use of the Nyberg-Rueppel signature scheme, the signature verification method takes as an input a pair (c,d') and includes the following five steps:

1) If c does not belong to the interval $[1,r-1]$, the signature is not valid;

2) Calculating the point $P=d'*2^{8t}.G+c.W$;

3) For j ranging from 0 to $2^{8t}-1$, executing the following steps:

3)a) If $P=O$, executing step 3)d);

3)b) Associating the integer i with the point P and calculating the integer $f=c-i$ modulo r;

3)c) Finding the message m from f and verifying that $f=R(m)$; if yes, executing step 5);

3)d) Replacing P with $P+G$;

4) The signature is not valid and the method is terminated;

5) If the integer $d=d'*2^{8t}+j$ does not belong to the interval $[0,r-1]$, the signature is not valid; otherwise the signature is valid and the method is terminated.

The sixth method of the invention consists of a modification of the Nyberg and Rueppel signature scheme making it possible to increase the messages to be signed by t bytes, t being an integer variable. The sixth method utilises a redundancy function R, an elliptic curve forming a group structure in which the zero element is denoted O and the point G on the curve, which point G is the generator of a sub-group of order a prime number r. The private key is a positive integer s less than r and the public key is the point

$W=s.G$. The method of generating the signature of a message m includes the following five steps:

1) Generating a random number u and calculating $V=u.G$;

2) Obtaining the message m' by removing from the message m the t least significant bytes and calculating $f=R(m')$;

3) Associating an integer i with the point V and calculating $c=i+f$ modulo r; returning to step 1) if $c=0$ and if i is not equal to m modulo 2^{8t};

4) Calculating $d=u-s*c$ modulo r;

5) The signature is the pair of integers (c,d).

The signature verification method includes the following four steps:

1) If c does not belong to the interval $[1,r-1]$ or if d does not belong to the interval $[0,r-1]$, the signature is not valid;

2) Calculating the point $P=d.G+c.W$; if $P=O$, the signature is not valid;

3) Associating the integer i with the point P and calculating the integer $f=c-i$ modulo r;

4) Finding the message m' from f and verifying that $f=R(m')$; if yes, finding the message m by concatenating the t least significant bytes of i with the message m'. The signature of the message m is then valid; otherwise the signature is not valid.

The seventh method of the invention consists of a modification of the signature scheme with partial reconstitution of the message described previously making it possible to increase by t bytes the size of the message m_1 reconstituted from the signature, t being an integer variable. The seventh method uses a redundancy function R, an elliptic curve forming a group structure in which the zero element is denoted O and a point G on the curve, which point G is the generator of a sub-group of order a prime number r. The private key is a positive integer s less than r and the public key is the point W=s.G. The method of generating the signature of a message m, consisting of two messages m_1 and m_2, includes the following six steps:

1) Generating a random integer u between 1 and r-1 and calculating V=u.G;

2) Obtaining m'_1 by removing the t least significant bytes from the message m_1. Calculating $f_1=R(m'_1)$;

3) Associating an integer i with the point V and calculating $c=i+f_1$ modulo r; if c=0 or if i is not equal to m_1 modulo 2^{8t}, returning to step 1;

4) Calculating $f_2=H(m_2)$, where H is a hash function;

5) Calculating the integer $d=u^{-1}*(f_2+s*c)$ modulo r; if d=0, returning to step 1;

6) The signature is the pair of integers (c,d).

The signature verification method takes as an input a pair of integers (c,d) and the partial message m_2 and comprises the following seven steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [1,r-1], the signature is not valid;

2) Calculating $f_2=H(m_2)$, where H is a hash function;

3) Calculating the integers $h=d^{-1}$ modulo r, $h_1=f_2*h$ modulo r and $h_2=c*h$ modulo r;

4) Calculating the point $P=h_1G+h_2W$; if P=O, this signature is not valid.

5) Associating the integer i with the point P;

6) Calculating the integer $f_1=c-i$ modulo r;

7) Obtaining the message m'_1 from f_1 and verifying that $f_1=R(m'_1)$; if yes, obtaining m_1 by concatenating the t least significant bytes of the integer i with the message m'_1. The signature of the message m is then valid; otherwise the signature is not valid.

It is possible, for the sixth and seventh methods, to reduce the calculation time by effecting preprocessing. Such preprocessing consists in putting in memory in a table pairs of integers (u,i) as defined previously so that these integers are accessible through the value of i modulo 2^{8t}.

The eighth method of the invention consists of a modification of the Nyberg and Rueppel signature scheme consisting in removing t bytes from the integer c previously defined, t being an integer variable. The signature generation method includes the following two steps:

1) Generating the signature of the message m using the Nyberg-Rueppel signature scheme in order to obtain the pair of integers (c,d);

2) Calculating c', the integer quotient of the division of the integer c by 2^{8t}. The signature is the pair of integers (c',d).

The signature verification method takes as an input the pair of integers (c',d) and includes the following five steps:

1) If d does not belong to the interval [0,r-1], the signature is not valid;

2) Calculating the point $P=d.G+c'*2^{8t}.W$;

3) For j ranging from 0 to $2^{8t}-1$, executing the following steps:

3)a) If P=O, executing step 3)d);

3)b) Associating the integer i with the point P and calculating the integer f=c-i modulo r;

3)c) Finding the message m from f and verifying that f=R(m); if yes, executing step 5);

3)d) Replacing P by P+W;

4) The signature is not valid and the method is terminated;

5) If the integer $c=c'*2^{8t}+j$ does not belong to the interval [1,r-1], the signature is not valid; otherwise the signature is valid and the method is terminated.

The ninth method of the invention is a modification of the signature scheme with partial reconstitution of the message defined previously, which consists in removing t bytes from the integer c defined previously, t being an integer variable. The signature generation method comprises the following two steps:

1) Generating the signature of the message m, consisting of two messages m_1 and m_2, using the signature scheme with partial reconstitution of the message in order to obtain the pair of integers (c,d);

2) Calculating c', the integer quotient of the division of the integer c by 2^{8t}. The signature is the pair of integers (c',d).

The signature verification method takes as an input a pair of integers (c',d) and a message m_2 and comprises the following eight steps:

1) If d does not belong to the interval [1,r-1], the signature is not valid;

2) Calculating $f_2=H(m_2)$, where H is a hash function;

3) Calculating the integers $h=d^{-1}$ modulo r, $h_1=f_2*h$ modulo r and $h_2=c'*2^{8t}*h$ modulo r;

4) Calculating the point $P=h_1.G+h_2.W$;

5) Calculating the point Z=h.W;

6) For j ranging from 0 to $2^{8t}-1$, executing the following steps:

6)a) If P=O, executing step 6)d);

6)b) Associating the integer i with the point P and calculating the integer $f_1=c-i$ modulo r;

6)c) Finding the message m_1 from f_1 and verifying that $f_1=R(m_1)$; if yes, executing step 8);

6)d) Replacing P with P+Z;

7) The signature is not valid and the method is terminated;

8) If the integer $c=c'*2^{8t}+j$ does not belong to the interval [1,r-1], the signature is not valid;

otherwise the signature is valid and the method is terminated.

The tenth method of the invention consists of a modification of the signature scheme with partial reconstitution of the message previously described, which consists in replacing the signature (c,d) with the signature (h_2,d) with $h_2=c*d^{-1}$ modulo r. The advantage of this tenth method is to allow a reduction in calculation time when this method is applied to any one of the previously defined methods.

The eleventh method of the invention consists of an improvement to the Nyberg-Rueppel signature scheme given previously, and consists in including part of the message of size t bytes in the integer d defined previously, t being a small integer, and using another redundancy function. In this method, the t least significant bytes of the integer d contain t bytes of the message. The eleventh method uses an elliptic curve forming a group structure in which the zero element is denoted O and a point G on the curve, which point G is the generator of a sub-group of order a prime number r. The private key is a positive integer s less than r and the public key is the point W=s.G. The method of generating the signature of a message m uses the integer parameters t, a and k and includes the following seven steps:

1) Calculating h=H(m), H being a hash function;

2) Removing the t least significant bytes and the k most significant bytes of the message m and storing the result in m';

3) Storing in f the result of the concatenation with m′ of the a most significant bytes of h;

4) Generating a random number u between 1 and r-1 and calculating V=u.G;

5) Associating an integer i with the point V and calculating c=i+f modulo r; returning to step 4) if c=0;

6) Calculating the integer d=u-s*c modulo r; if d is not equal to m modulo 2^{8t} returning to step 4);

7) The signature is the pair of integers (c,d).

The signature verification method includes the following seven steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [0,r-1], the signature is not valid;

2) Calculating the point P=d.G+c.W; if P=O, the signature is not valid;

3) Associating the integer i with the point P;

4) Calculating the integer f=c-i modulo r;

5) Concatenating the t least significant bytes of d with the message m′ obtained from f by removing the a least significant bytes;

6) For b ranging from 0 to 2^{8k}-1, repeating the following step:

6)a) Concatenating the message m′ with b in order to obtain m and calculating h=H(m); verifying that the a most significant bytes of h and the a least significant bytes of f are identical; if yes, the signature of the message m is valid and the method is terminated;

7) The signature is not valid.

The methods described therefore make it possible to significantly reduce the total size of the signature and of the message to be transmitted. When the memory space is limited, it is thus possible to store a larger number of signatures. In addition, it is also possible to effect a more rapid transmission of the signatures. These methods are particularly intended to be set up in portable devices, for example of the smart card type.

CLAIMS

1. An electronic signature method comprising a generation method and a verification method allowing total reconstitution of the message, the said method utilising a redundancy function R, a set having a group structure of order a prime number r, with a zero element denoted O and generating the point G, the private key being a positive integer less than r, the public key being the point $W=s.G$, the said method using a non-zero integer constant k, characterised in that the signature generation method includes the following four steps:

1) Generating a random number u between 1 and r-1 and calculating $V=u.G$;

2) Associating an integer i with the point V and calculating $c=i+f$ modulo r; if $c=0$, returning to step 1);

3) Calculating the integer $d=u^{-1}*(k+s*c)$ modulo r; if $d=0$, returning to step 1);

4) The signature is the pair of integers (c,d);

and in that the signature verification method includes the following six steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [1,r-1], the signature is not valid;

2) Calculating the integers $h = d^{-1}$ modulo r, $h_1=k*h$ modulo r and $h_2=c*h$ modulo r;

3) Calculating the point $P = h_1G + h_2W$; if $P=0$, the signature is not valid;

4) Associating an integer i with the point P;

5) Calculating the integer f=c-i modulo r;

6) Finding the message m from f and verifying that f=R(m); if yes, the signature of the message m is valid; otherwise the signature is valid.

2. An electronic signature method comprising a generation method and a signature verification method allowing partial reconstruction of the message, the message m to be signed being divided into two parts, the first part m_1 of constant size being reconstituted from the signature, the second part m_2 being transmitted with the signature of the method, the said method utilising a redundancy function R, a set having a group structure of order a prime number r, with a zero element denoted O and generating the point G, the private key being a positive integer less than r and the public key being the point W=s.G, characterised in that the method of generating the signature of a message m consisting of the messages m_1 and m_2 includes the following six steps:

1) Generating a random integer u between 1 and r-1 and calculating V=u.G;

2) Calculating $f_1=R(m_1)$;

3) Associating an integer i with the point V and calculating $c=i+f_1$ modulo r; if c=0, returning to step 1;

4) Calculating $f_2=H(m_2)$, where H is a hash function;

5) Calculating the integer $d=u^{-1}*(f_2+s*c)$ modulo r; if d=0, returning to step 1;

6) The signature is the pair of integers (c,d);

and in that the signature verification method takes as an input a pair of integers (c,d) and the partial message m_2 and comprises the following seven steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [1,r-1], the signature is not valid;

2) Calculating $f_2=H(m_2)$, where H is a hash function;

3) Calculating the integers $h=d^{-1}$ modulo r, $h_1=f_2*h$ modulo r and $h_2=c*h$ modulo r;

4) Calculating the point $P=h_1G+h_2W$; if P=0, the signature is not valid;

5) Associating the integer i with the point P;

6) Calculating the integer $f_1=c-i$ modulo r;

7) Obtaining the message m_1 from f_1 and verifying that $f_1=R(m_1)$; if yes, the signature of the message m is valid; otherwise the signature is not valid.

3. An electronic signature method comprising a generation method and a signature verification method characterised in that it consists in including part of the message inside the signature by suitably choosing the random data used during the generation of the signature.

4. An electronic signature method comprising a generation method and a signature verification method, characterised in that it consists in eliminating some of the bytes representing the signature, the complete

reconstitution of the signature taking place during the verification phase.

5. A method for improving the Nyberg-Rueppel signature scheme according to Claim 3, comprising a generation method and a verification method and consisting in including part of the message of size t bytes in the integer d, t being a small integer, the signature being the pair of integers (c,d), the t least significant bytes of the integer g containing t bytes of the message, the said method using a redundancy function R, a set having a group structure of order a prime number r, with a zero element denoted O and generating the point G, the private key being a positive integer s less than r and the public key being the point W=s.G, characterised in that the method of generating the signature of a message m includes the following five steps:

1) Removing the t least significant bytes of the message m and storing the result in m'; calculating f=R(m');

2) Generating a random number u between 1 and r-1 and calculating V=u.G;

3) Associating an integer i with the point V and calculating c=i+f modulo r; returning to step 1) if c=0.

4) Calculating the integer d=u-s*c modulo r; if d is not equal to m modulo 2^{8t}, returning to step 2);

5) The signature is the pair of integers (c,d);

and in that the signature verification method includes the following five steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [0,r-1], the signature is not valid;

2) Calculating the point P=d.G+c.W; if P=0, the signature is not valid;

3) Associating the integer i with the point P;

4) Calculating the integer f=c-i modulo r;

5) Obtaining the message m′ from f and verifying that f=R(m′); if such is not the case, the signature is not valid; if such is the case, the signature is valid and the message m is the concatenation with the message m′ of the t least significant bytes of the integer d.

6. A method for the preprocessing of the signature generation according to Claim 5, making it possible to accelerate the generation of the signatures, the said method comprising a pretreatment phase and a signature generation phase, the said pretreatment phase taking as an input the secret key s and consisting in putting in memory in a table a large number of values (i, x_u) with x_u=u-s*i modulo r and i being the integer associated with the point V=u.G, so that these values can be accessed by the remainder of x_u modulo 2^{8t}, the said signature generation phase utilising a redundancy function R, a set having a group structure of order a prime number r, with a zero element denoted O and generating the point G, the private key being a positive integer s less than r and the public key being the point W=s.G, the said signature generation phase being characterised by the following eight steps:

1) Removing the t least significant bytes in the message m and storing the result in the message m'; calculating f=R(m'). The t least significant bytes of the message m are stored in the integer δ;

2) Calculating the integer $y=s*f$ modulo r and the integer $\lambda=y$ modulo 2^{8t};

3) If $y<r/2$, first of all executing step 4 and next step 5; otherwise executing first of all step 5 and next step 4;

4) Accessing the elements of the table where the remainder modulo 2^{8t} is $\lambda+\delta$ modulo 2^{8t} and selecting an element such that x_u is greater than or equal to y; if such an element exists, it is eliminated from the table and the method passes to step 6);

5) Accessing the elements of the table where the remainder modulo 2^{8t} is $\lambda+\delta+r$ modulo 2^{8t} and selecting an element such that x_u is less than y; if such an element exists, it is eliminated from the table and the method passes to step 6);

6) Calculating the integer $d=x_u-y$ modulo r;

7) Obtaining the integer i associated with x_u and calculating $c=i+f$ modulo r;

8) The signature is the pair of integers (c,d).

7. A method for improving the signature scheme with partial reconstitution of the message according to Claim 2, the said method comprising a signature generation method and a signature verification method, the said method consisting in including part of the message of size t bytes in the integer d defined

previously, t being a small integer, the t least significant bytes of the integer d containing t bytes of the message, the said method utilising a redundancy function R, a set having a group structure of order a prime number r, with a zero element denoted O and generating a point G, the private key being a positive integer less than r and the public key being the point W=s.G, characterised in that the method of generating the signature of a message m consisting of the messages m_1 and m_2 includes the following six steps:

1) Generating a random integer u between 1 and r-1 and calculating V=u.G;

2) Calculating $f_1=R(m_1)$;

3) Associating an integer i with the point V and calculating $c=i+f_1$ modulo r; if c=0, returning to step 1;

4) Calculating $f_2=H(m_2)$, where H is a hash function;

5) Calculating the integer $d=u^{-1}*(f_2+s*c)$ modulo r; if d=0 or if d is not equal to m_2 modulo 2^{8t}, returning to step 1;

6) The signature is the pair of integers (c,d) and the message to be transmitted is m'_2 consisting of m_2 deprived of its t least significant bytes;

and in that the signature verification method takes as an input a pair of integers (c,d) and the partial message m'_2 and comprises the following eight steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [1,r-1], the signature is not valid;

2) Making up m'_2 as m_2 by adding to it the t least significant bytes of d;

3) Calculating $f_2=H(m_2)$, where H is a hash function;

4) Calculating the integers $h=d^{-1}$ modulo r, $h_1=f_2*h$ modulo r and $h_2=c*h$ modulo r;

5) Calculating the point $P=h_1G+h_2W$; if P=0 the signature is not valid;

6) Associating the integer i with the point P;

7) Calculating the integer $f_1=c-i$ modulo r;

8) Obtaining the message m_1 from $f_1$and verifying that $f_1=R(m_1)$; if yes, the signature of the message m is valid; otherwise the signature is not valid.

8. A method consisting in removing t bytes from the chain of bytes representing the integer d when the signature is the pair of integers (c,d), the said method comprising a signature generation method and a signature verification method, the said method being applied to the Nyberg and Rueppel signature scheme, characterised in that the modified signature generation method includes the following two steps:

1) Generating the signature of the message m using the Nyberg and Rueppel signature scheme, to obtain the pair of integers (c,d);

2) Calculating d', the integer quotient of the division of the integer d by 2^{8t}; the signature is the pair of integers (c,d');

and in that the modified signature verification method takes as an input a pair (c,d') and includes the following five steps:

1) If c does not belong to the interval [1,r-1], the signature is not valid;

2) Calculating the point $P=d'*2^{8t}.G+c.W$;

3) For j ranging from 0 to $2^{8t}-1$, executing the following steps:

3)a) If P=O, executing step 3)d);

3)b) Associating the integer i with the point P and calculating the integer f=c-i modulo r;

3)c) Finding the message m from f and verifying that f=R(m); if yes, executing step 5);

3)d) Replacing P with P+G;

4) The signature is not valid and the method is terminated;

5) If the integer $d=d'*2^{8t}+j$ does not belong to the interval [0,r-1], the signature is not valid; otherwise the signature is valid and the method is terminated.

9. A method consisting in removing t bytes from the chain of bytes representing the integer d when the signature is the pair of integers (c,d), the said method comprising a signature generation method and a signature verification method, the said method to the signature diagram with partial reconstitution of the message according to Claim 2, characterised in that the modified signature generation method includes the following two steps:

1) Generating the signature of the message m using the signature scheme with partial reconstruction of the message previously described, in order to obtain the pair of integers (c,d);

2) Calculating d', the integer quotient of the division of the integer d by 2^{8t}; the signature is the pair of integers (c,d');

and in that the modified signature verification method takes as an input a pair (c,d') and a message m_2 and includes the following two steps:

1) For i ranging from 0 to $2^{8t}-1$, calculating the integer $d=d'*2^{8t}+i$ and executing the signature verification method with partial reconstitution of the message previously described, the signature to be verified being (c,d); if the signature verification method recognises the signature (c,d) as valid, the signature is valid, and the method is terminated;

2) The signature is not valid.

10. A method for improving the Nyberg and Rueppel scheme making it possible to increase the size of the messages to be signed by t bytes, t being an integer variable, the said method comprising a signature generation method and a signature verification method, the said method utilising a redundancy function R, a set having a group structure of order a prime number r, with a zero element denoted O and generating the point G, the private key being a positive integer s less than r and the public key being the point W=s.G, characterised in that the method of generating the

signature of a message m includes the following five steps:

1) Generating a random number u and calculating V=u.G;

2) Obtaining the message m' by removing from the message m the t least significant bytes and calculating f=R(m');

3) Associating an integer i with the point V and calculating c=i+f modulo r; returning to step 1) if c=0 and if i is not equal to m modulo 2^{8t};

4) Calculating d=u-s*c modulo r;

5) The signature is the pair of integers (c,d);

and in that the signature verification method includes the following four steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [0,r-1], the signature is not valid;

2) Calculating the point P=d.G+c.W; if P=O, the signature is not valid;

3) Associating the integer i with the point P and calculating the integer f=c-i modulo r;

4) Finding the message m' from f and verifying that f=R(m'); if yes, finding the message m by concatenating the t least significant bytes of i with the message m'. The signature of the message m is then valid; otherwise the signature is not valid.

11. A method for improving the signature scheme with partial reconstitution of the message according to Claim 2, the said method comprising a signature generation method and a signature verification method,

the said method making it possible to increase by t bytes the size of the message m_1 reconstituted from the signature, t being an integer variable, said method utilising a redundancy function R, a set having a group structure of order a prime number r, with a zero element denoted O and generating the point G, the private key being a positive integer less than r and the public key being the point W=s.G, characterised in that the method of generating the signature of a message m includes the following six steps:

1) Generating a random integer u between 1 and r-1 and calculating V=u.G;

2) Obtaining m'_1 by removing the t least significant bytes from the message m_1. Calculating $f_1=R(m'_1)$;

3) Associating an integer i with the point V and calculating $c=i+f_1$ modulo r; if c=0 or if i is not equal to m_1 modulo 2^{8t}, returning to step 1;

4) Calculating $f_2=H(m_2)$, where H is a hash function;

5) Calculating the integer $d=u^{-1}*(f_2+s*c)$ modulo r; if d=0, returning to step 1;

6) The signature is the pair of integers (c,d);

and in that the signature verification method takes as an input a pair of integers (c,d) and the partial message m_2 and comprises the following seven steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [1,r-1], the signature is not valid;

2) Calculating $f_2=H(m_2)$, where H is a hash function;

3) Calculating the integers $h=d^{-1}$ modulo r, $h_1=f_2*h$ modulo r and $h_2=c*h$ modulo r;

4) Calculating the point $P=h_1G+h_2W$; if P=O, this signature is not valid.

5) Associating the integer i with the point P;

6) Calculating the integer $f_1=c-i$ modulo r;

7) Obtaining the message m'_1 from f_1 and verifying that $f_1=R(m'_1)$; if yes, obtaining m_1 by concatenating the t least significant bytes of the integer i with the message m'_1. The signature of the message m is then valid; otherwise the signature is not valid.

12. A method for preprocessing the calculations making it possible to increase the performances of the methods according to Claims 10 and 11, characterised in that it consists in putting in memory in a table pairs of integers (u,i) as defined previously so that these integers are accessible to the value of i modulo 2^{8t}, t being an integer parameter.

13. A method for improving the Nyberg and Rueppel signature scheme consisting in removing t bytes from the integer c, t being an integer variable, the said method comprising a signature generation method and a signature verification method, the signature consisting of the pair of integers (c,d), characterised in that the signature generation method includes the following two steps:

1) Generating the signature of the message m using the Nyberg-Rueppel signature scheme in order to obtain the pair of integers (c,d);

2) Calculating c', the integer quotient of the division of the integer c by 2^{8t}. The signature is the pair of integers (c',d);

and in that the signature verification method takes as an input the pair of integers (c',d) and includes the following five steps:

1) If d does not belong to the interval [0,r-1], the signature is not valid;

2) Calculating the point $P=d.G+c'*2^{8t}.W$;

3) For j ranging from 0 to $2^{8t}-1$, executing the following steps:

3)a) If P=O, executing step 3)d);

3)b) Associating the integer i with the point P and calculating the integer f=c-i modulo r;

3)c) Finding the message m from f and verifying that f=R(m); if yes, executing step 5);

3)d) Replacing P by P+W;

4) The signature is not valid and the method is terminated;

5) If the integer $c=c'*2^{8t}+j$ does not belong to the interval [1,r-1], the signature is not valid; otherwise the signature is valid and the method is terminated.

14. A method for improving the signature scheme with partial reconstitution of the message according to Claim 2, consisting in removing t bytes from the integer c defined according to Claim 2, t being an

integer variable, the said method comprising a signature generation method and a signature verification method, characterised in that the signature generation method comprises the following two steps:

1) Generating the signature of the message m, using the signature scheme with partial reconstitution of the message in order to obtain the pair of integers (c,d);

2) Calculating c', the integer quotient of the division of the integer c by 2^{8t}; the signature is the pair of integers (c',d);

and in that the signature verification method takes as an input a pair of integers (c',d) and a message m_2 and comprises the following eight steps:

1) If d does not belong to the interval [1,r-1], the signature is not valid;

2) Calculating $f_2=H(m_2)$, where H is a hash function;

3) Calculating the integers $h=d^{-1}$ modulo r, $h_1=f_2*h$ modulo r and $h_2=c'*2^{8t}*h$ modulo r;

4) Calculating the point $P=h_1.G+h_2.W$;

5) Calculating the point $Z=h.W$;

6) For j ranging from 0 to $2^{8t}-1$, executing the following steps:

6)a) If $P=O$, executing step 6)d);

6)b) Associating the integer i with the point P and calculating the integer $f_1=c-i$ modulo r;

6)c) Finding the message m_1 from f_1 and verifying that $f_1=R(m_1)$; if yes, executing step 8);

6)d)Replacing P with P+Z;

7) The signature is not valid and the method is terminated;

8) If the integer $c=c'*2^{8t}+j$ does not belong to the interval [1,r-1], the signature is not valid; otherwise the signature is valid and the method is terminated.

15. A method for modifying the signature scheme with partial reconstruction of the message according to any one of the preceding claims, characterised in that it consists in replacing the signature (c,d) with the signature (h_2,d) with $h_2=c*d^{-1}$ modulo r.

16. A method for improving the Nyberg-Rueppel signature scheme, said method comprising a signature generation method and a signature verification method, the said method consisting in including part of the message of size t bytes in the integer d, the signature being the pair of integers (c,d), t being a small integer, the t least significant bytes of the integer d containing t bytes of the message, the said method utilising a set having a group structure of order a prime number r, with a zero element denoted O and generating the point G, the private key being a positive integer s less than r and the public key being the point W=s.G, characterised in that the method of generating the signature of a message m using the integer parameters t, a and k includes the following seven steps:

1) Calculating h=H(m), H being a hash function;

2) Removing the t least significant bytes and the k most significant bytes of the message m and storing the result in m';

3) Storing in f the result of the concatenation with m' of the a most significant bytes of h;

4) Generating a random number u between 1 and r-1 and calculating V=u.G;

5) Associating an integer i with the point V and calculating c=i+f modulo r; returning to step 4) if c=0;

6) Calculating the integer d=u-s*c modulo r; if d is not equal to m modulo 2^{8t} returning to step 4);

7) The signature is the pair of integers (c,d);

and in that the signature verification method includes the following seven steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [0,r-1], the signature is not valid;

2) Calculating the point P=d.G+c.W; if P=O, the signature is not valid;

3) Associating the integer i with the point P;

4) Calculating the integer f=c-i modulo r;

5) Concatenating the t least significant bytes of d with the message m' obtained from f by removing the a least significant bytes;

6) For b ranging from 0 to 2^{8k}-1, repeating the following step:

6)a) Concatenating the message m' with b in order to obtain m and calculating h=H(m); verifying that the a most significant bytes of h and the a least significant bytes of f are identical; if yes, the signature of the message m is valid and the method is terminated;

7) The signature is not valid.

17. A method for generating and verifying an electronic signature according to any one of the preceding claims, characterised in that the operations are effected on an elliptic curve forming a group structure and having at least one point G, which is the generator of a sub-group of order a prime number r.

18. A method for generating and verifying an electronic signature according to any one of the preceding claims, characterised in that the operations are effected in the multiplicative group of the integers modulo a prime number p.

19. A method for generating and verifying an electronic signature according to any one of the preceding claims, characterised in that the operations are effected in a multiplicative sub-group of order a prime number r of the multiplicative group of the integers modulo a prime number p with r dividing p-1.

20. An electronic device according to any one of the preceding claims, characterised in that the device performing the test is a portable device.

21. An electronic device according to any one of the preceding claims, characterised in that the device is a smart card.

22. An electronic device according to any one of the preceding claims, characterised in that the device is a contactless card.

23. An electronic device according to any one of the preceding claims, characterised in that the device is a PCMCIA card.

24. An electronic device according to any one of the preceding claims, characterised in that the device is a badge.

25. An electronic device according to any one of the preceding claims, characterised in that the device is an intelligent watch.

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international

(43) Date de la publication internationale
8 février 2001 (08.02.2001)

PCT

(10) Numéro de publication internationale
WO 01/10078 A1

(51) Classification internationale des brevets[7]: H04L 9/32

(21) Numéro de la demande internationale: PCT/FR00/02024

(22) Date de dépôt international: 12 juillet 2000 (12.07.2000)

(25) Langue de dépôt: français

(26) Langue de publication: français

(30) Données relatives à la priorité:
99/10106 30 juillet 1999 (30.07.1999) FR

(71) Déposant *(pour tous les États désignés sauf US)*: GEMPLUS [FR/FR]; Parc d'activités de Gémenos, Avenue du Pic de Bertagne, F-13881 Gémenos (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(pour US seulement)*: **CORON, Jean-Sébastien** [FR/FR]; 4, rue Léon de Lagrange, F-75015 Paris (FR). **NACCACHE, David** [FR/FR]; 7, rue Chaptal, F-75009 Paris (FR). **STERN, Jacques** [FR/FR]; 7, rue Pierre Nicole, F-75005 Paris (FR).

(74) Mandataire: **BRUYERE, Pierre**; Gemplus, Parc d'activités de Gémenos, Avenue du Pic de Bertagne, F-13881 Gémenos (FR).

(81) États désignés *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) États désignés *(régional)*: brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée:
— *Avec rapport de recherche internationale.*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) Title: SIGNATURE SCHEMES BASED ON DISCRETE LOGARITHM WITH PARTIAL OR TOTAL MESSAGE RECOVERY

(54) Titre: SCHEMAS DE SIGNATURE A BASE DE LOGARITHME DISCRET AVEC RECONSTITUTION PARTIELLE OU TOTALE DU MESSAGE

(57) Abstract: The invention concerns signature scheme methods whereof the security is based on the discrete logarithm problem, a first scheme for total recovery of the message, a second scheme for partial recovery of the message. The invention also concerns two techniques for reducing to a minimum the total size of the message to be transmitted and of the signature. The first technique consists in including part of the message inside the signature by appropriately selecting the random data used when the signature is generated. The second technique consists in eliminating part of the octets representing the signature, the total recovery of the signature being obtained during the second verification phase. Said schemes and said two techniques aim at reducing the overall size of the signature and of the message to be transmitted. They are therefore particularly designed to be used on portable media such as smart cards.

(57) Abrégé: L'invention consiste en des procédés de schéma de signature dont la sécurité est basée sur le problème du logarithme discret, un premier schéma permettant une reconstitution totale du message, un deuxième schéma permettant une reconstitution partielle du message. L'invention consiste également en deux techniques permettant de minimiser la taille totale du message à transmettre et de la signature. La première technique consiste à inclure une partie du message à l'intérieur de la signature en choisissant convenablement les données aléatoires utilisées lors de la génération de la signature. La deuxième technique consiste à supprimer une partie des octets représentant la signature, la reconstitution complète de la signature s'effectuant durant la phase de vérification. Ces schémas et ces 2 techniques ont pour but de réduire la taille totale de la signature et du message à transmettre. Ils sont donc particulièrement destinés à être utilisés sur des supports portables de type carte à puce.

032326-192
Attorney's Docket No.

COMBINED DECLARATION AND POWER OF ATTORNEY FOR UTILITY OR DESIGN PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SIGNATURE SCHEMES BASED ON DISCRETE LOGARITHM WITH PARTIAL OR TOTAL MESSAGE RECOVERY

the specification of which (**check only one item below**):

☒ is attached hereto.

□ was filed as United States Patent application
Number _____ on _____
and was amended on _____ (if applicable).

☒ was filed as PCT International application
Number PCT/FR00/02024 on 12 July 2000
and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §§ 119 (a)-(d), 172 or 365 of any foreign application(s) for patent or inventor's certificate or of any international (PCT) application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international (PCT) application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

PRIOR FOREIGN/PCT APPLICATION(S) AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. §§119(a)-(d), 172 or 365:			
COUNTRY (if PCT, indicate "PCT")	APPLICATION NUMBER	DATE OF FILING (day, month, year)	PRIORITY CLAIMED UNDER 35 U.S.C. §§119, 172 or 365
France	99/10106	30 July 1999	☒Yes □No

Combined Declaration and Power of Attorney
for Utility or Design Patent Application
Attorney's Docket No. 032326-192
Page 2 of 4

I hereby appoint the following attorneys and agent(s) to prosecute said application and to transact all business in the U.S. Patent and Trademark Office connected therewith and to file, prosecute and to transact all business in connection with international applications directed to said invention:

William L. Mathis	17,337	Eric H. Weisblatt	30,505	Bruce T. Wieder	33,815
Robert S. Swecker	19,885	James W. Peterson	26,057	Todd R. Walters	34,040
Platon N. Mandros	22,124	Teresa Stanek Rea	30,427	Ronni S. Jillions	31,979
Benton S. Duffett, Jr.	22,030	Robert E. Krebs	25,885	Harold R. Brown III	36,341
Norman H. Stepno	22,716	William C. Rowland	30,888	Allen R. Baum	36,086
Ronald L. Grudziecki	24,970	T. Gene Dillahunty	25,423	Brian P. O'Shaughnessy	32,747
Frederick G. Michaud, Jr.	26,003	Patrick C. Keane	32,858	Kenneth B. Leffler	36,075
Alan E. Kopecki	25,813	B. Jefferson Boggs, Jr.	32,344	Fred W. Hathaway	32,236
Regis E. Slutter	26,999	William H. Benz	25,952	Wendi L. Weinstein	34,456
Samuel C. Miller, III	27,360	Peter K. Skiff	31,917	Mary Ann Dillahunty	34,576
Robert G. Mukai	28,531	Richard J. McGrath	29,195	Donna M. Meuth	36,607
George A. Hovanec, Jr.	28,223	Matthew L. Schneider	32,814	Mark R. Kresloff	42,766
James A. LaBarre	28,632	Michael G. Savage	32,596	21839	
E. Joseph Gess	28,510	Gerald F. Swiss	30,113		
R. Danny Huntington	27,903	Charles F. Wieland III	33,096		

and: ______

Address all correspondence to:

James A. LaBarre
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404

21839

Address all telephone calls to: James A. LaBarre at (703) 836-6620.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

FULL NAME OF SOLE OR FIRST INVENTOR	Jean-Sebastien CORON
Signature	
Date	29/02/2002
Residence (City, State, Country)	Paris, France FRX
Citizenship	French
Mailing Address	4, rue Leon de Lagrange, F-75015, Paris, France
City, State, ZIP, Country	F-75015, Paris, France
FULL NAME SECOND INVENTOR, IF ANY	David NACCACHE
Signature	David Naccache
Date	31/1/02
Residence (City, State, Country)	Paris, France FRX
Citizenship	French
Mailing Address	7, rue, Chaptal, F-75009, Paris, France
City, State, ZIP, Country	F-75009, Paris, France

Combined Declaration and Power of Attorney
for Utility or Design Patent Application
Attorney's Docket No. 032326-192
Page 3 of 3

38

FULL NAME OF THIRD INVENTOR, IF ANY	Jacques STERN
Signature	
Date	25/02/2002
Residence (City, State, Country)	Paris, France FRX
Citizenship	French
Mailing Address	7, rue Pierre, Nicole, F-75005, Paris, France
City, State, ZIP, Country	F-75005, Paris, France
FULL NAME OF FOURTH INVENTOR, IF ANY	
Signature	
Date	
Residence (City, State, Country)	
Citizenship	
Mailing Address	
City, State, ZIP, Country	
FULL NAME OF FIFTH INVENTOR, IF ANY	
Signature	
Date	
Residence (City, State, Country)	
Citizenship	
Mailing Address	
City, State, ZIP, Country	
FULL NAME OF SIXTH INVENTOR, IF ANY	
Signature	
Date	
Residence (City, State, Country)	
Citizenship	
Mailing Address	
City, State, ZIP, Country	
FULL NAME OF SEVENTH INVENTOR, IF	
Signature	
Date	
Residence (City, State, Country)	
Citizenship	
Mailing Address	
City, State, ZIP, Country	